Getting Ready for the NIST Threshold Call

Threshold Call

NISTIR 8214C ipd

Threshold Workshop

MPTS 2023 (Sep-26–28)

Presented* on August 22nd @ Crypto 2023 Rump Session

* Luís Brandão: At NIST as a Foreign Guest Researcher (non-employee), Contractor from Strativia.
Expressed opinions are from the speaker and should not be construed as official NIST views. Joint work with René Peralta.

Outline

1. The “Threshold Call”
2. The “Threshold Workshop” (MPTS 2023)
3. Timeline

Outline

1. The “Threshold Call”
2. The “Threshold Workshop” (MPTS 2023)
3. Timeline

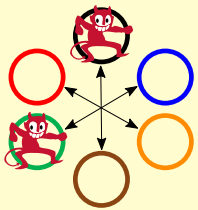
NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) $\Rightarrow$ Final version (**late 2023**).
- Submission deadline (expected $\approx$ **2nd-half 2024**)

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Final version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)

Calling for submissions of threshold schemes

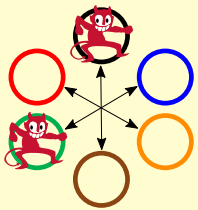


(And gadgets for modular use)

Presented at
Crypto 2023
Rump Session

NIST Call for Multi-Party Threshold Schemes

- NISTIR 8214C: Initial public **draft** (**Jan 2023**) ⇒ Final version (**late 2023**).
- Submission deadline (expected ≈ **2nd-half 2024**)



Calling for submissions of threshold schemes for:

- **[Cat1] Selected NIST-standardized primitives**
- **[Cat2] Other primitives (including FHE, IBE/ABE, ZKP)**

  (And gadgets for modular use)

FHE = Fully-homomorphic encryption.
IBE/ABE = Identity/Attribute-based encryption.
ZKP = Zero-knowledge proof.

Presented at
Crypto 2023
Rump Session

More about the Call

Submission components: (1) Written specification; (2) Reference implementation (open source); (3) Execution instructions; (4) Experimental evaluation; (5) Statements.

Received 12 initial public comments (April 2023): Thank you!

Positive impact in the revision. Comments at: https://csrc.nist.gov/pubs/ir/8214/c/ipd

Various expected revisions: refine subcategories, e.g., inc. NIST-selected PQC; ...

Wide scope: pre- and post-quantum; also welcome work from other SDOs.

Presented at
Crypto 2023
Rump Session

Assorted notes about the process

- **Setup:** A gathering of reference material (not a competition for a selection).
- **Expected:** The process will clarify relevant system models, best practices, ...
- **Aim:** Devise recommendations about advanced cryptography (PEC + MPTC)
  (Will support future standardization processes.)

  PEC = Privacy-Enhancing Crypto
  MPTC = Multi-Party Threshold Crypto
- **Ample room for participation:** Give feedback → Submit → Analyze
- **It's time:** Consider starting to organize a future submission (team, scope, ...)

Presented at
Crypto 2023
Rump Session

Outline

1. The “Threshold Call”
2. The “Threshold Workshop” (MPTS 2023)
3. Timeline

Threshold Workshop (MPTS 2023)

Workshop on Multi-Party Threshold Schemes (MPTS) 2023

- **When:** **September 26–28** (submit by **September 5th**)
- **Format:** Fully virtual; short presentations (mostly 5–15 min)
- **Attendance:** Free (upon simple registration)
- **Content:** comments to improve the Call/Process and community participation

Threshold Workshop (MPTS 2023)

Workshop on Multi-Party Threshold Schemes (MPTS) 2023

- **When:** **September 26–28** (submit by **September 5th**)
- **Format:** Fully virtual; short presentations (mostly 5–15 min)
- **Attendance:** Free (upon simple registration)
- **Content:** comments to improve the Call/Process and community participation

Come hear/share technical nuggets of wisdom and motivation about the Threshold Call and Process

Presented at
Crypto 2023
Rump Session

Should you propose a presentation? Yes!

Submit by **Sep 5th** an abstract for a short presentation.

Call for abstracts

Should you propose a presentation? Yes!

Call for abstracts

Submit by **Sep 5th** an abstract for a short presentation.

Example suitable presentations:

1. Express interest in possibly submitting a threshold scheme (**in 2024**).
2. Give suggestions for improving the threshold call (NISTIR 8214C).
3. Explain a technical challenge in some subcategory of the Call.
4. Offer technical suggestions for the community of potential submitters.
5. For community awareness, reiterate previously submitted comments.

Presented at
Crypto 2023
Rump Session

Other suggested topics for presentations

Check the Workshop Call

1. **Scope of the Threshold Call:** refinements to the description of subcategories.
2. **Submission requirements:** clarifications needed in the Threshold Call (NISTIR 8214C ipd).
3. **Expressions of interest:** intended concrete submissions (and possible team).
4. **Need and adoptability:** special features/primitives useful for specific apps.
5. **Inspiration:** suggestions to the community, for submission of concrete threshold schemes.
6. **Frameworks:** pertinent system models, security formulations, threshold parameters.
7. **Pre/post quantum:** pre-quantum and post-quantum cases worth focusing on.
8. **Technical challenges:** regarding concrete primitives / threshold schemes / assumptions.
9. **External efforts:** other processes developing related reference material / specifications.

http://csrc.nist.gov/events/2023/mpts2023

Outline

Tentative timeline

- **2023-Sep-26–28:** Virtual **workshop** for feedback & awareness
- **Late 2023:** **Final** version of the call
- **2nd half of 2024:** Deadline for **submissions** of threshold schemes / gadgets
- **2024/2025:** **Workshop(s)** for characterization/analysis of submitted schemes
- $\geq$ **2025:** Initial **recommendations** (and start new processes?)

Presented at
Crypto 2023
Rump Session

Thank you for your attention!

Getting Ready for the NIST Threshold Call

Presented at Crypto 2023 Rump Session | August 22nd @ Santa Barbara (USA)

- MPTC-forum: https://csrc.nist.gov/projects/threshold-cryptography/email-list
- PEC-forum: https://csrc.nist.gov/projects/pec/email-list

Threshold Call

Threhsold Workshop